REMARKS

Claims 1-5, 9-22, 24-29 and 32 are currently pending in the subject application and are presently under consideration. Claims 1 and 5 have been amended as shown on pages 2-3 of the Reply. Claim 10 has been cancelled herein, and claims 6-8, 23, 30, and 31 were cancelled previously. These amendments add no new matter to the claims, nor do they change the scope of the claims as previously presented. Rather, independent claim 1 has been amended to incorporate the subject matter of claim 10, which has been duly cancelled. The amendments therefore do not introduce an additional search burden. Entry and consideration of these amendments is therefore respectfully requested.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-5, 9-16, and 32 Under 35 U.S.C. §102(e)

Claims 1-5, 9-16, and 32 are rejected under 35 U.S.C. §102(e) as allegedly being anticipated by Batke, *et al.* (U.S. Patent 7,536,548). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Batke, *et al.* does not disclose or suggest each and every feature set forth in the subject claims.

> For a prior art reference to anticipate, 35 U.S.C. §102 requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

The present application relates generally to network and automation device security in an industrial automation environment. To this end, one or more automation security protocols can be provided that facilitate secure operations and communications within a control or factory environment (see, *e.g.*, paragraph [0009]). In one example, protocol extensions can also be adapted to factory networks. In particular, protocol or packet extensions can be provided in association with factory protocols, such as extending path information within a Control and Information Protocol (CIP) to include a *who* segment to identify or authenticate a requester or supplier of the connection (see, *e.g.*, paragraphs [0012] - [0014]). This can take the form of an

encrypted identification, certificate, public key, or other process to identify the requester (see, *e.g.*, paragraph [0050]). In particular, amended independent claim 1 recites, *an extensible factory protocol comprising a* ***Control and Information Protocol (CIP) having a path segment adapted to include a segment identifying a requestor of a connection*** *between automation assets and employed to authenticate the requestor.*

Contrary to assertions made in the Office Action, Batke, *et al.* does not disclose or suggest these features. Batke, *et al.* relates to a network security system for use in an industrial control environment, wherein security layers can be configured within an industrial controller, and the security layer can be associated with one or more security components to control or restrict data access to the controller (see Abstract). Arguing that Batke, *et al.* discloses a CIP protocol having a path segment adapted to include a segment identifying a requestor of a connection, the Office Action notes in particular that the security layers described in the cited reference can provide machine authentication and user encryption, and that network protocols such as CIP can be encapsulated within an encrypted transmission stream (column 2, lines 50-67 and lines 35-49).

However, Batke, *et al.* does not indicate that this machine authentication is achieved *via* a *CIP protocol having a path segment adapted to include a segment identifying a requester of a connection*, and indeed the cited reference does not contemplate adapting a path segment of a CIP protocol in this fashion. Moreover, although the Examiner notes that Batke, *et al.* can encapsulate a CIP protocol within a security packet, such an encapsulation does not involve *adapting a path segment of the CIP protocol to include a segment identifying a requester.* Rather, the exemplary encapsulation protocol described in Batke, *et al.* - the SSL Handshake Protocol discussed at column 6, lines 6-13 - enables two communicating systems to authenticate each other and to negotiate an encryption algorithm and cryptographic keys *before an application protocol transmits or receives its first byte of data.* Thus, since the encapsulation method of Batke, *et al.* performs its authentication before an application protocol begins transmitting data, the encapsulation does not involve an *adaptation of the application protocol itself*, and in particular does not involve adapting a path segment of a CIP protocol to include a segment identifying a requestor. This is underscored at column 6, lines 10-11of Batke, *et al.*, which states that "an advantage of SSL is that it is *application protocol independent*" (emphasis added). The protocol independence of the encapsulation described in Batke, *et al.* implies that

no modification of a path segment of the protocol itself is required. Thus, it is submitted that Batke, *et al.* does not disclose or suggest *an extensible factory protocol comprising a* ***Control and Information Protocol (CIP) having a path segment that has been adapted to include a segment identifying a requestor of a connection*** *between automation assets and employed to authenticate the requestor*, as recited in amended independent claim 1.

In view of at least the foregoing, it is respectfully submitted that Batke, *et al.* does not disclose or suggest each and every feature of amended independent claim 1 (and all claims depending there from), and as such fails to anticipate or render obvious the present application. It is therefore requested that this rejection be withdrawn.

II. Rejection of Claims 1-5, 9-16, and 32 Under 35 U.S.C. §102(e)

Claims 1-5, 9-16, and 32 are rejected under 35 U.S.C. §102(e) as allegedly being anticipated by Salowey (U.S. Patent 7,370,350). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Salowey does not disclose or suggest each and every feature of the subject claims.

As noted *supra*, Batke, *et al.* does not disclose or suggest *an extensible factory protocol comprising a* ***Control and Information Protocol (CIP) having a path segment adapted to include a segment identifying a requestor of a connection*** *between automation assets and employed to authenticate the requestor*, as recited in amended independent claim 1. While conceding that Salowey also fails to disclose these aspects, the Office Action asserts that Braatz, *et al.* cures these deficiencies (page 14 of the Office Action, discussing claim 10, which has been incorporated into independent claim 1). Braatz, *et al.* relates to a system for network-enabling electrical and electronic devices using device-independent and device-dependent access controllers. This system comprises a device-independent access controller (DIAC) and a device-dependent access controller (DDAC) coupled to a network, wherein the DIAC and the DDAC can communicate over the network using a communication protocol. This communication protocol supports a set of device-dependent commands, carried onboard the DDAC, which allow the DIAC access to the device functionality set (see paragraph [0014]). Communication between the DIAC and a DDAC is achieved using a proprietary protocol called Object Control Interface Protocol (OCIP), which passes datasets between the DIAC and the DDAC (see paragraph [0118]). The Office Action asserts that this OCIP protocol reads on the CIP protocol adapted as

set forth in amended independent claim 1, noting in particular that the OCIP includes a header with fields that identify the destination and source devices of a communication (Figure 6).

However, as disclosed at paragraphs [0118] and [0245] of Braatz, *et al.*, this OCIP protocol is a *proprietary* protocol designed to work within the context of the cited network-enabling system. Since OCIP is proprietary, and particular to the system described in Braatz, *et al.* (as opposed to the open industrial protocol of CIP), the fact that this proprietary protocol includes a source device field in its header does not suggest a *CIP* protocol having *a path segment adapted to include a segment identifying a requestor of a connection between automation assets*. By providing such an adapted CIP protocol, one or more embodiments of the present application can cleanly integrate security mechanisms within a control-specific factory network environment. Braatz, *et al.*, alone or in combination with Salowey, does not provide this benefit.

In view of at least the foregoing, it is respectfully submitted that Salowey and Braatz, *et al.*, individually or in combination, do not disclose or suggest all aspects of amended independent claim 1 (and all claims depending there from), and as such fail to make obvious the present application. It is therefore respectfully requested that this rejection be withdrawn.

III. Rejection of Claim 10 Under 35 U.S.C. §103(a)

Claim 10 is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Salowey, in view of Braatz, *et al.* (U.S. 2002/0120728). However, claim 10 has been cancelled, and the subject matter thereof has been incorporated into independent claim 1, as discussed *supra*. Withdrawal of this rejection is therefore respectfully requested.

IV. Rejection of Claims 17-24 Under 35 U.S.C. §103(a)

Claims 17-24 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Salowey, in view of Brandstad, *et al.* (U.S. Patent 6,842,860). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Salowey and Brandstad, *et al.*, individually or in combination, do not disclose or suggest all aspects set forth in the subject claims.

According to one or more embodiments of the present application, security protocols can be applied to a plurality of network situations and can be determined, altered, and adjusted based

upon system performance or security considerations. For example, during real-time communications between remote devices and an automation asset, lighter weight security protocols can be employed to transmit data between network components, where lighter weight refers to the number of security data or extensions that may be provided or associated with a data packet that also are employed to mitigate impact on system performance (see, *e.g.*, paragraph [0028]). Additionally, time-based components can be encoded within the security protocols, including security time-outs after a predetermined amount of time has passed, thus causing a subsequent determination or security negotiation before further data transactions can be achieved (see, *e.g.*, paragraph [0034]. These time-based components can take the form of time-limited data encoded within the security protocol such as a clock value indicating how long a communication session or data transfer can last or has time remaining to transmit or receive data before having to renegotiate for further data transactions (see, *e.g.*, paragraph [0047]). In particular, independent claim 17 recites, *providing a security time-out within the wireless security protocol that times-out data transactions between the automation devices after a predetermined time duration until a subsequent determination of real-time data transfer requirements and network security requirements is performed.*

The Office Action contends that Branstad, *et al.* discloses these time-out features. Branstad, *et al.* relates to an authentication mechanism wherein a message authentication code is applied only to some portions of the message in order to improve speed of transmission (see Abstract). An ACSA (adaptive cryptographically synchronized authentication) controller determines which authentication mechanism should be used in providing authentication for data exchanged between nodes sharing a given security association (see column 4, lines 24-28). Asserting that Branstad, *et al.* discloses the security time-out functionality of independent claim 17, the Office Action indicates the heartbeat interval parameter described in that reference. According to column 6, lines 8-11 of Branstad, *et al.*, this heartbeat interval parameter is "a timeout interval during which an ASCA participant *should expect to receive a control message* from the remote party" (emphasis added). The functionality of this heartbeat interval is further described at column 8, lines 46-67 of the cited reference, in connection with a coordinated "gear switch" operation between a sender and a receiver (that is, a change in the security mechanism employed for communications between the sender and receiver, based on respective processor loads). Specifically, column 8, lines 46-49 of Branstad, *et al.* states:

> "On the receiver's side, the process begins at step 720, when the receiver receives a gear switch message [from the sender]. *Before the expiration of the heartbeat interval, the receiver...then returns a gear switch acknowledgement message*." (emphasis added)

The consequences of a failure to receive this acknowledgement at the sender within the heartbeat interval are described at column 8, lines 64-67:

> "On the other side, *the sender will eventually switch back to the base gear*, either upon receipt of the synchronization failure message *or upon lack of receipt of the heartbeat message within the heartbeat interval*." (emphasis added)

Thus, contrary to assertions made in the Office Action, the heartbeat interval of Branstad, *et al.* does not *time-out* data transactions between automation devices after a predetermined time duration until a subsequent determination of real-time data transfer requirements and network security requirements is performed. Rather, according to the passages cited above, the heartbeat interval represents a *time allowance for receipt of an anticipated control message*, expiration of which interval causes the sender to *switch back to a base security mechanism.* No data transactions are timed out as a result of this switch in security mechanisms. Indeed, attempting to equate the heartbeat interval of Branstad, et al. with the security time-out of independent claim 17 in the *Response to Arguments* section, the Office Action qualifies this interpretation by stating that Branstad, *et al.* "uses the heartbeat interval to timeout *non-base gear* data transactions when the heartbeat interval lapses without a gear switch acknowledgement message" (emphasis added). This appears to be an admission that Branstad, *et al.* does not time-out *data transactions* generally, but rather "times-out" the use of a non-base gear security mechanism for data transactions. This reversion to a base gear security mechanism does not result in a time-out of *data transactions*. Rather, data transactions are continued under a different security mechanism. As such, Branstad, *et al.* fails to disclose or suggest a security time-out that *times-out data transactions between automation devices after a predetermined time duration until a subsequent determination of real-time data transfer requirements and network security requirements is performed.*

Salowey is also silent regarding such a security time-out. Salowey relates to a method of authenticating a first computing device in communication over a network to a second computing device using an Extensible Authentication Protocol (EAP). According to this method, the first computing device is authenticated to the second computing device using a first authentication mechanism. Short-term re-authentication data is generated and issued to the first computing device. Later, a request from the first computing device to re-authenticate to the second computing device is received. The first re-authentication device is then re-authenticated to the second computing device by presenting the short-term authentication credential to the second computing device (see Abstract). However, Salowey does not select encryption mechanisms based on a determination of data transfer requirements, and therefore does not contemplate a security time-out that enforces making such determinations, as set forth in independent claim 17.

Similarly, independent claim 20 recites, *providing a security time-out within the security protocol that times-out the communications session after a predetermined amount of time until a subsequent determination for real-time communication is made.* As discussed above, neither Salowey nor Branstad, *et al.* discloses or suggest these aspects.

Likewise, independent claim 24 recites, *means for enforcing a time limit on data exchange between the automation asset in the control domain and the automation asset remote to the domain, after which time limit the data exchange is timed-out until the performance parameter is re-determined.* The cited references are silent regarding such a time limit, as noted *supra.*

In view of at least the foregoing, it is respectfully submitted that Salowey and Branstad, *et al.*, individually or in combination, do not disclose or suggest all features of independent claims 17, 20 and 24 (and all claims depending there from), and as such fail to make obvious the present application. Withdrawal of this rejection is therefore respectfully requested.

V. Rejection of Claims 25-29 Under 35 U.S.C. §103(a)

Claims 25-29 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Salowey, in view of Branstad, *et al.*, and further in view of Bridges, *et al.* (AI Techniques Applied to High Performance Computing Intrusion Detection"). However, independent claim 25 recites, *a time component encoded in the factory protocol that defines an amount of time after which data exchange between control devices is timed-out until the at least one of a security or*

performance parameter is re-evaluated. As discussed *supra*, Salowey and Branstad, *et al.* are silent regarding such a time component. Bridges, *et al.* does not cure these shortcomings. Bridges, *et al.* relates to the use of artificial intelligence techniques in intrusion detection mechanisms, but does not disclose or suggest encoding a time component within a factory protocol that *defines an amount of time after which data exchange between control devices is timed-out until a security or performance parameter is re-evaluated*, as provided in independent claim 25.

Also, independent claim 28 recites, *providing a time-based component within the industrial network protocol that defines an amount of time after which the real-time performance must be re-evaluated before data transactions between the automation devices are allowed to continue*, and as discussed above, none of the cited references disclose or suggest these aspects.

In view of at least the foregoing, it is respectfully submitted that Salowey and Branstad, *et al.*, individually or in combination, do not disclose or suggest all features set forth in amended independent claims 25 and 28 (and all claims depending there from), and as such fail to render obvious the present application. It is therefore requested that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USB].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

TUROCY & WATSON, LLP

/Brian Steed/
Brian Steed
Reg. No. 64,095

TUROCY & WATSON, LLP
127 Public Square
57th Floor, Key Tower
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731